

# PATENT COOPERATION TREATY


## PCT

### INTERNATIONAL PRELIMINARY EXAMINATION REPORT (PCT Article 36 and Rule 70)

REC'D 30 AUG 2005

WIPO

PCT

Applicant's or agent's file reference CH920030006		<b>FOR FURTHER ACTION</b> See Notification of Transmittal of International Preliminary Examination Report (Form PCT/PEA/416)	
International application No. PCT/IB 03/05328	International filing date (day/month/year) 20.11.2003	Priority date (day/month/year) 30.05.2003	
International Patent Classification (IPC) or both national classification and IPC H04L29/06			
Applicant INTERNATIONAL BUSINESS MACHINES CORPORATION et al.			
<p>1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of 7 sheets, including this cover sheet.</p> <p><input checked="" type="checkbox"/> This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).</p> <p>These annexes consist of a total of 1 sheets.</p>			
<p>3. This report contains indications relating to the following items:</p> <ul style="list-style-type: none"> <li>I <input checked="" type="checkbox"/> Basis of the opinion</li> <li>II <input type="checkbox"/> Priority</li> <li>III <input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</li> <li>IV <input type="checkbox"/> Lack of unity of invention</li> <li>V <input checked="" type="checkbox"/> Reasoned statement under Rule 66.2(a)(II) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</li> <li>VI <input type="checkbox"/> Certain documents cited</li> <li>VII <input type="checkbox"/> Certain defects in the international application</li> <li>VIII <input type="checkbox"/> Certain observations on the international application</li> </ul>			
Date of submission of the demand 02.12.2004		Date of completion of this report 29.08.2005	
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465		Authorized Officer  Kopp, K  Telephone No. +49 89 2399-7833	



# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/IB 03/05328

## I. Basis of the report

1. With regard to the **elements** of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)*):

### Description, Pages

1, 3-13 as originally filed  
2 filed with telefax on 07.07.2005

### Claims, Numbers

1-22 as originally filed

### Drawings, Sheets

1/4-4/4 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

**INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT**

International application No. **PCT/IB 03/05328**

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

*(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)*

6. Additional observations, if necessary:

**V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Yes: Claims	1-22
	No: Claims	
Inventive step (IS)	Yes: Claims	
	No: Claims	1-22
Industrial applicability (IA)	Yes: Claims	1-22
	No: Claims	

2. Citations and explanations

**see separate sheet**

**INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/IB 03/05328

**Re Item V**

**Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Reference is made to the following documents (D):

- D1: WO 02/061510 A (COPELAND JOHN A III ;LANCOPE INC (US)) 8 August 2002 (2002-08-08)
- D2: US 2002/156898 A1 (POIRIER DANIEL EARL ET AL) 24 October 2002 (2002-10-24)
- D3: WO 02/086724 A (RECOURSE TECHNOLOGIES INC) 31 October 2002 (2002-10-31)
- D4: WO 02/03653 A (BRITISH TELECOMM ;SOPPERA ANDREA (IT)) 10 January 2002 (2002-01-10)
- D5: US 2002/105910 A1 (BRANDON KEVIN WILLIAM ET AL) 8 August 2002 (2002-08-08)

2. Claim 1 lacks an inventive step (Article 33(3) PCT).

Document D1, which is considered to represent the most relevant state of the art for claim 1, discloses insofar the subject-matter is clear, according to the subject-matter of claim 1:

- A method for detecting attacks on a data communications network having a plurality of addresses for assignment to data processing systems in the network (page 6, lines 14-16); the method comprising:
- identifying data traffic on the network (page 6, lines 22-23);
- inspecting any data traffic so identified for data indicative of an attack (page 6, lines 30-31); and,
- on detection of data indicative of an attack, generating an alert signal (page 6, line 31 - page 7, line 2).

The subject-matter of claim 1 differs from the disclosure in D1 in that:

- the identified data traffic is originated from any assigned address and addressed to any unassigned address.

This difference is however without inventive significance for the following reasons: inspecting data traffic for data indicative of an attack is consuming more resources

**INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/IB 03/05328

than inspecting a subset of the data traffic.

However, choosing a subset of data to be inspected, e.g. inspecting only data traffic originated from a group of source addresses and addressed to free addresses, i.e. inspecting data traffic originated from any assigned address to any unassigned address, is a common design measure obvious for a person skilled in the art.

3. The above finding also applies to independent claims 8, 15, 16 and 21 which correspond to independent claim 1.
4. Dependent claims do not contain any subject-matter which, in combination with the subject-matter to which they refer, meets the requirements of the PCT in respect of inventive step (Articles 33(3) PCT). They are either disclosed in D2-D5 (e.g. "rerouting any data traffic originating at the address assigned to the data processing system originating the data indicative of the attack to an address on the network", "providing a report to said entity containing information related to one of alert, ...") or common measures (e.g. "the alert message comprises data indicative of the attack detected") obvious for a person skilled in the art.
5. Certain defects in the international application
  - 5.1 The features of the claims should have been provided with reference signs placed in parentheses (Rule 6.2(b) PCT).
  - 5.2 The independent claims should have been formulated in the two-part form in accordance with Rule 6.3(b) PCT, with those features known in combination from the prior art document D1 being placed in the preamble (Rule 6.3(b)(I) PCT) and with the remaining features being included in the characterising part (Rule 6.3(b)(ii) PCT).
  - 5.3 The relevant background art disclosed in the document D1 should have been mentioned and identified in the description (Rule 5.1(a)(ii) PCT).
6. Certain observations in the international application, i.e. the claims do not meet the requirements of Article 6 PCT:
  - 6.1 Although method claims 1 and 21 and apparatus claims 8 and 15 have been

**INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/IB 03/05328

drafted as separate independent claims, they appear to relate effectively to the same subject-matter and to differ from each other only with regard to the definition of the subject-matter for which protection is sought and in respect of the terminology used for the features of that subject-matter. The aforementioned claims therefore lack conciseness.

**6.2 The expressions**

- "technical data" used in claim 20;
- "the degree of network security achieved" used in claim 19;
- "the turnover of said entity" used in claim 19;

are vague and unclear and leave the reader in doubt as to the meaning of the technical features to which they refer, thereby rendering the definition of the subject-matter of said claims unclear.

**6.3 The subject-matter of claim 7 is unclear, since the formulation "comprising including in the warning message program code" is not clear.**

**6.4 The scope of protection sought for of claim 15 is unclear, since the data communications network is not defined per se but only specified by its relationship to a second entity "a plurality of addresses for assignment to data processing system" and a third entity "apparatus for detecting attacks on the network". In addition, there is no link between the second and third entity in order to solve a technical problem.**

**6.5 The scope of protection sought for of claim 16 is unclear, since it is not clear if the processor is configured to perform all of the method steps or not as claimed in claims 1 to 7.**

**6.6 An antecedent definition for the expressions**

- "the warning message program code" in claim 7;
  - "the warning message" in claim 14;
  - "the charge being billed", "said entity", "the size of the network", "the number of unassigned addresses", the number of assigned addresses", the volume of data traffic", the number of attacks", the number of alerts", "the signature of the identified attack", the volume of rerouted data traffic", "the degree of network security achieved", "the turnover of said entity" in claim 19;
  - "the attack-handling" in claim 20;
- is missing.

**INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT - SEPARATE SHEET**

---

International application No. PCT/IB 03/05328

- 6.7 As explained below, some of the features in the apparatus claims 9, 11, 16 relate to a method of using the apparatus rather than clearly defining the apparatus in terms of its technical features. The intended limitations are therefore not clear from these claims:
- "inspects" in claim 9;
  - "sends" in claim 11;
  - "configures" in claim 16.
- 6.8 The subject-matter of claim 13 is unclear, since it is not clear of how to assign a disinfection server to the disinfection address. However it is clear of how to assign the disinfection address to the disinfection server.
- 6.9 The expression "preferably", used in claim 19 leads to doubts about the scope of protection (PCT Guidelines 5.40), because it is unclear if the features following this expression is part of the scope of protection sought for or not.
- 6.10 The backreference of claim 5 leads to doubts about the scope of protection sought for: said claim is referenced to itself.
- 6.11 According to Rule 6.4(c) PCT, all claims referring back to a single previous claim, shall be grouped together, which is not the case for claims 17-20, which are referenced back on claim 1.

CH920030006

2

~~/New page 2 (Shall replace former page 2)/~~

processing system usually referred to as a router. In operation, the router directs inbound communication traffic from the Internet to specified IP addresses on the network.

Similarly, the router directs outbound communication traffic from the network in the direction of specified IP addresses on the Internet.

A problem faced by many ISPs is the increasing frequency of electronic attacks to the networks they operate. Such attacks include computer virus attacks and so-called "worm" attacks. Attacks of this nature introduce significant performance degradation in networks operated by ISPs. Infected systems connected to the network typically attempt to spread the infection within the network. Many users do not recognize that their systems are infected. It would be desirable to provide technology for triggering disinfection of such systems in the interests of increasing network performance.

#### Summary of the Invention

In accordance with the present invention, there is now provided a method for detecting attacks on a data communications network having a plurality of addresses for assignment to data processing systems in the network, the method comprising: identifying data traffic on the network originating at any assigned address and addressed to any unassigned address; inspecting any data traffic so identified for data indicative of an attack; and, on detection of data indicative of an attack, generating an alert signal.

The term "unassigned" herein is meant as covering an address that is not assigned to a physical device other than an apparatus for detecting an intrusion or generating an attack signature. In other words, the term unassigned is meant as covering an address which is free, i.e. not assigned to user systems. The apparatus that is designed to execute the method according to the invention will be the device those "unassigned" addresses are actually assigned to in order to make use of the invention. Those addresses are insofar unassigned as they are